ForeScout

CounterACT 7.0

Einzelne CounterACT-Appliance

Kurzanleitung für die Installation

Inhaltsverzeichnis

Willkommen zu CounterACT™ Version 7.0 3
Lieferumfang Ihres CounterACT-Pakets 3

Überblick 4

1. Erstellen eines Bereitstellungsplans 5
Auswählen des Bereitstellungsorts für die Appliance 5
Verbindungen der Appliance-Schnittstelle 5

2. Einrichten Ihres Switches 8
A. Verbindungsoptionen für den Switch 8
B. Hinweise zur Switchkonfiguration 9

3. Anschließen der Netzwerkkabel und erste Schritte 11
A. Auspacken der Appliance und Anschließen der Kabel 11
B. Notieren der Schnittstellenzuweisungen 12
C. Einschalten der Appliance 12

4. Konfigurieren der Appliance 13

5. Remoteverwaltung 16
iDRAC7-Einrichtung 16

6. Prüfen der Verbindungen 21
Prüfen der Verbindung zur Verwaltungsschnittstelle 21
Prüfen der Verbindung zwischen Switch und Appliance 21
Durchführen des Pingtests 22

7. Einrichten von CounterACT Console 23
Installieren von CounterACT Console 23
Anmelden 24
Durchführen der Anfangseinstellungen 24

Kontaktinformationen 26

Willkommen zu CounterACT™ Version 7.0

Mit der NAC-Lösung (Network Access Control, Netzwerkzugriffsteuerung) von ForeScout erhalten Kunden die vollständige Kontrolle über die Sicherheit ihres Netzwerks, ohne die Produktivität des Unternehmens und der Endbenutzer einzuschränken. CounterACT kombiniert modernste NAC-Technik mit Technologien zur Vorbeugung von Angriffen in einer einzigen Appliance. CounterACT führt eine vollständige Endpunktüberprüfung und Zugriffsteuerung jedes Netzwerkgeräts durch - und kann nahtlos in jede bestehende IT-Infrastruktur integriert werden.

In diesem Handbuch wird die Installation einer einzelnen, eigenständigen CounterACT-Appliance erläutert.

Nähere Einzelheiten oder Informationen zur Bereitstellung mehrerer Appliances für unternehmensweiten Netzwerkschutz erhalten Sie im *CounterACT Installation Guide (CounterACT-Installationshandbuch)* und dem *Console User Manual (CounterACT Console-Benutzerhandbuch)*. Diese Dokumente stehen auf der CounterACT-CD im Verzeichnis „/docs“ zur Verfügung.

Darüber hinaus haben Sie über die Support-Website unter „http://www.forescout.com/support“ Zugriff auf die neusten Dokumentationen, Artikel in der Wissensdatenbank und Aktualisierungen für Ihre Appliance.

Lieferumfang Ihres CounterACT-Pakets

- CounterACT-Appliance
- Kurzanleitung für die Installation
- CounterACT-CD mit Console-Software, CounterACT Console-Benutzerhandbuch und CounterACT-Installationshandbuch
- Garantieunterlagen
- Montagehalterungen
- Netzkabel
- Anschlusskabel für die DB9-Konsole (nur für seriellen Anschluss)

Überblick

Zum Einrichten von CounterACT sind die folgenden Schritte erforderlich:

1. Erstellen eines Bereitstellungsplans
2. Einrichten Ihres Switches
3. Anschließen der Netzwerkkabel und erste Schritte
4. Konfigurieren der Appliance
5. Remoteverwaltung
6. Prüfen der Verbindungen
7. Einrichten von CounterACT Console

1. Erstellen eines Bereitstellungsplans

Vor der Installation sollten Sie überlegen, wo die Appliance bereitgestellt werden soll. Zudem sollten Sie sich mit den Anschlüssen an der Appliance-Schnittstelle vertraut machen.

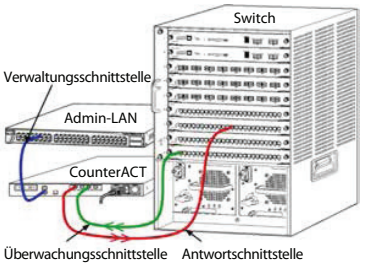
Auswählen des Bereitstellungsorts für die Appliance

Die Auswahl des richtigen Netzwerkstandorts für die Installation der Appliance ist von entscheidender Bedeutung für eine erfolgreiche Bereitstellung und eine optimale Leistung von CounterACT. Der geeignete Standort ist abhängig von Ihren jeweiligen Implementierungszielen und der gewünschten Netzwerkzugriffsrichtlinie. Die Appliance sollte in der Lage sein, den Datenverkehr zu überwachen, der für die gewünschte Richtlinie relevant ist. Wenn Ihre Richtlinie beispielsweise auf einer Überwachung der Autorisierungsereignisse zwischen den Endpunkten und den Authentifizierungsservern des Unternehmens beruht, muss die Appliance so installiert werden, dass sie auf den Datenverkehr zwischen Endpunkt(en) und Authentifizierungsserver(n) zugreifen kann.

Weitere Informationen zu Installation und Bereitstellung erhalten Sie im CounterACT-Installationshandbuch (CounterACT Installation Guide), das sich auf der im Lieferumfang dieses Pakets enthaltenen CounterACT-CD befindet.

Verbindungen der Appliance-Schnittstelle

Die Appliance verfügt im Allgemeinen über drei Verbindungen zum Netzwerkswitch.



Verwaltungsschnittstelle

Über diese Schnittstelle können Sie CounterACT verwalten sowie Anfragen und weitreichende Überprüfungen der Endpunkte durchführen. Die Schnittstelle muss mit einem Switchport verbunden sein, der Zugriff auf alle Endpunkte im Netzwerk ermöglicht.

Jede Appliance benötigt eine eigene Verwaltungsverbindung zum Netzwerk. Für diese Verbindung ist eine IP-Adresse im lokalen LAN sowie der Zugriff auf den TCP-Port 13000 von den Computern aus erforderlich, auf denen die CounterACT Console-Verwaltungsanwendung ausgeführt wird. Die Verwaltungsschnittstelle muss auf die folgenden Komponenten Ihres Netzwerks zugreifen können:

Port	Service	Von oder zu CounterACT	Funktion
TCP 22	SSH	Zu	Ermöglicht Zugriff auf die CounterACT-Befehlszeilenschnittstelle.
TCP 2222			(Hochverfügbarkeit) Ermöglicht Zugriff auf physische CounterACT-Geräte, die zum Hochverfügbarkeitscluster gehören. Verwenden Sie den TCP-Port 22, um auf die gemeinsame (virtuelle) IP-Adresse des Clusters zuzugreifen.

Port	Service	Von oder zu CounterACT	Funktion
445/139	RPC	Von	Ermöglicht CounterACT die Durchführung einer umfassenden Untersuchung und Kontrolle von Windows-Endpunkten mit Hilfe von RPC.
135	WMI	Von	Ermöglicht CounterACT die Durchführung einer umfassenden Untersuchung und Kontrolle von Windows-Endpunkten mit Hilfe von WMI.
10003	Secure Connector	Zu	Ermöglicht SecureConnector die Herstellung einer sicheren (mit SSL verschlüsselten) Verbindung zwischen Appliance und Windows-Computern. Über diese Verbindung empfängt und beantwortet SecureConnector Anfragen für Überprüfungen und Aktionen. Der gesamte CounterACT-Datenverkehr zwischen SecureConnector und der Appliance wird über die sichere Verbindung übertragen.
TCP 2200	Secure Connector	Zu	Ermöglicht SecureConnector die Herstellung einer sicheren (mit SSH verschlüsselten) Verbindung zwischen Appliance und Macintosh-/Linux-Computern. SecureConnector stellt den Zugriff auf nicht verwaltete Endpunkte über ein Shellskript bereit, dass auf dem Desktop ausgeführt wird, während der Host mit dem Netzwerk verbunden ist.
22	SSH	Von	Ermöglicht CounterACT die Durchführung einer umfassenden Untersuchung und Kontrolle von Macintosh- und Linux-Endpunkten.
TCP 25	SMTP	Von	Dienst zum Senden von E-Mails aus CounterACT.
TCP 80	HTTP	Zu	Ermöglicht HTTP-Umleitungen.
TCP 443	HTTPS	Zu	Ermöglicht HTTP-Umleitungen über SSL.
TCP 13000	CounterACT	Zu	Ermöglicht Verbindungen zwischen Console und Appliance. In Systemen mit mehreren CounterACT-Appliances sind zudem Verbindungen zwischen Console und Enterprise Manager sowie zwischen Enterprise Manager und jeder Appliance möglich.
UDP 53	DNS	Von	Ermöglicht CounterACT die Auflösung interner IP-Adressen.
UDP 123	NTP	Von	Ermöglicht CounterACT den Zugriff auf einen NTP-Zeitserver. CounterACT verwendet standardmäßig ntp.foreScout.net.
UDP 161	SNMP	Von	Ermöglicht CounterACT die Kommunikation mit Komponenten der Netzwerkinfrastruktur, wie z. B. Switches und Router. Weitere Informationen zur Konfiguration von SNMP erhalten Sie im *CounterACT Console User Manual (CounterACT Console-Benutzerhandbuch).*

UDP 162	SNMP	Zu	Ermöglicht CounterACT den Empfang von SNMP-Traps von Komponenten der Netzwerkinfrastruktur, wie z. B. Switches und Router. Weitere Informationen zur Konfiguration von SNMP erhalten Sie im *CounterACT Console User Manual (CounterACT Console-Benutzerhandbuch)*.

Überwachungsschnittstelle

Diese Verbindung ermöglicht die Überwachung und Nachverfolgung des Netzwerkdatenverkehrs durch die Appliance.

Der Datenverkehr wird zu einem Port am Switch gespiegelt und von der Appliance überwacht. Je nach Anzahl der zu spiegelnden VLANs wird für den Datenverkehr VLAN-Tagging gemäß 802.1Q genutzt.

- **Einzelnes VLAN („untagged"):** Wenn der überwachte Datenverkehr von einem einzelnen VLAN stammt, ist für den gespiegelten Datenverkehr kein VLAN-Tagging erforderlich.
- **Mehrere VLANs („tagged"):** Wenn der überwachte Datenverkehr von mehr als einem VLAN stammt, *muss* für den gespiegelten Datenverkehr VLAN-Tagging gemäß 802.1Q verwendet werden.

Wenn zwei Switches als redundantes Paar miteinander verbunden sind, muss die Appliance den Datenverkehr von beiden Switches überwachen.

In der Regel benötigt die Überwachungsschnittstelle keine IP-Adresse.

Antwortschnittstelle

Über diese Schnittstelle beantwortet die Appliance den Datenverkehr. Der Antwortdatenverkehr dient dem Schutz vor schädlichen Aktivitäten und zur Durchführung von Aktionen im Rahmen der NAC-Richtlinie. Zu diesen Aktionen gehören beispielsweise die Umleitung von Webbrowsern oder die Blockierung durch eine Firewall. Die damit verbundene Konfiguration des Switchports ist abhängig vom zu überwachenden Datenverkehr.

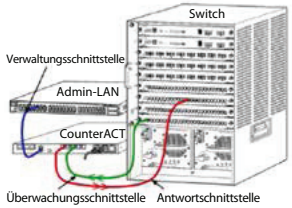
- **Einzelnes VLAN („untagged"):** Wenn der überwachte Datenverkehr aus einem einzigen VLAN stammt, muss die Antwortschnittstelle so konfiguriert werden, dass sie zum selben VLAN gehört. In diesem Fall benötigt die Appliance eine einzige IP-Adresse in diesem VLAN.
- **Mehrere VLANs („tagged"):** Wenn der überwachte Datenverkehr aus mehr als einem VLAN stammt, muss für die entsprechenden VLANs auf der Antwortschnittstelle VLAN-Tagging gemäß 802.1Q aktiviert werden. Die Appliance benötigt dann eine IP-Adresse für jedes geschützte VLAN.

2. Einrichten Ihres Switches

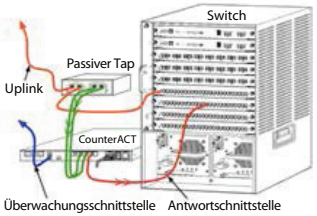
A. Verbindungsoptionen für den Switch

Die Appliance wurde so entwickelt, dass sie nahtlos in eine Vielzahl von Netzwerkumgebungen integriert werden kann. Für eine erfolgreiche Integration der Appliance in Ihrem Netzwerk müssen Sie sicherstellen, dass Ihr Switch für die Überwachung des benötigten Datenverkehrs entsprechend eingerichtet ist. Ihnen stehen verschiedene Optionen zur Verfügung, um eine Verbindung zwischen Appliance und Switch herzustellen.

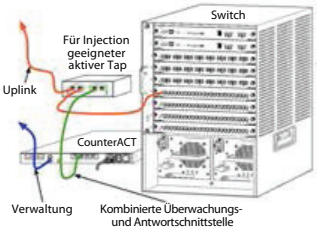
1. **Standardbereitstellung (separate Schnittstellen für Verwaltung, Überwachung und Antwort)**
   Bei der empfohlenen Bereitstellungsart werden drei separate Ports verwendet. Diese Ports werden im Abschnitt *„Verbindungen der Appliance-Schnittstelle" genauer erläutert*.



2. **Passiver Inline-Tap**
   Statt die Verbindung zu einem Überwachungsport am Switch herzustellen, kann die Appliance auch einen Inline-Tap verwenden. Ein passiver Tap erfordert zwei Überwachungsports, es sei denn, es werden „Rekombinations-Taps" verwendet. In diesem Fall werden die beiden Duplexströme in einem einzigen Port zusammengefasst. Die Konfiguration des Datenverkehrs muss für den Port mit Tap und die Antwortschnittstelle identisch sein. Wenn für den Datenverkehr an dem Port mit Tap beispielsweise VLAN-Tagging (gemäß 802.1Q) genutzt wird, muss die Antwortschnittstelle ebenfalls als Port mit VLAN-Tagging konfiguriert sein.



3. **Aktiver (für Injection geeigneter) Inline-Tap**
   Wenn die Appliance einen Inline-Tap verwendet, der *für Injection geeignet* ist, können die Schnittstellen für Überwachung und Antwort zusammengefasst werden. Die Konfiguration eines separaten Antwortports am Switch ist dann nicht erforderlich. Diese Option kann für jede Art von Upstream- oder Downstream-Switchkonfiguration verwendet werden.



4. **Antwort über IP-Layer (für Installationen mit Layer-3-Switches)** Die Appliance kann ihre eigene Verwaltungsschnittstelle für die Beantwortung des Datenverkehrs nutzen. Obwohl diese Option für jeden überwachten Datenverkehr geeignet ist, wird sie für Situationen empfohlen, in denen die Überwachungsports der Appliance zu keinem VLAN gehören und die Appliance deshalb nicht über einen beliebigen anderen Switchport auf den überwachten Datenverkehr antworten kann. Dies ist in der Regel der Fall, wenn ein Link zwischen zwei Routern überwacht wird.

   Diese Option kann keine Anfragen über das Address Resolution Protocol (ARP) beantworten, sodass die Fähigkeit der Appliance zur Erkennung von Scanvorgängen, die auf IP-Adressen im überwachten Subnetz abzielen, eingeschränkt ist. Diese Einschränkung entfällt, wenn der Datenverkehr zwischen zwei Routern überwacht wird.

B. Hinweise zur Switchkonfiguration

VLAN-Tagging (gemäß 802.1Q)

- **Überwachung eines einzelnen VLAN (Datenverkehr „untagged“)** Wenn der überwachte Datenverkehr aus nur einem einzigen VLAN stammt, ist kein VLAN-Tagging gemäß 802.1Q erforderlich.
- **Überwachung mehrerer VLANs (Datenverkehr „tagged“)** Wenn der überwachte Datenverkehr aus zwei oder mehr VLANs stammt, muss für Überwachungs- *und* Antwortschnittstelle VLAN-Tagging gemäß 802.1Q aktiviert werden. Die Option für die Überwachung mehrerer VLANs wird empfohlen, weil sie die beste Abdeckung gewährleistet und gleichzeitig die Anzahl der zur Spiegelung erforderlichen Ports minimiert wird.
- Wenn der Switch kein VLAN-Tagging gemäß 802.1Q an den zur Spiegelung verwendeten Ports nutzen kann, wählen Sie eine der folgenden Möglichkeiten:
  - Spiegeln eines einzigen VLAN
  - Spiegeln eines einzelnen Uplink-Ports („untagged“)
  - Verwenden der Option für Antwort über IP-Layer
- Wenn der Switch nur einen Port spiegeln kann, nutzen Sie für die Spiegelung einen einzigen Uplink-Port. Auf diesem kann VLAN-Tagging aktiviert werden. Wenn der Switch die VLAN-Tags gemäß 802.1Q entfernt, müssen Sie im Allgemeinen die Option zur Antwort über den IP-Layer verwenden.

Sonstiges

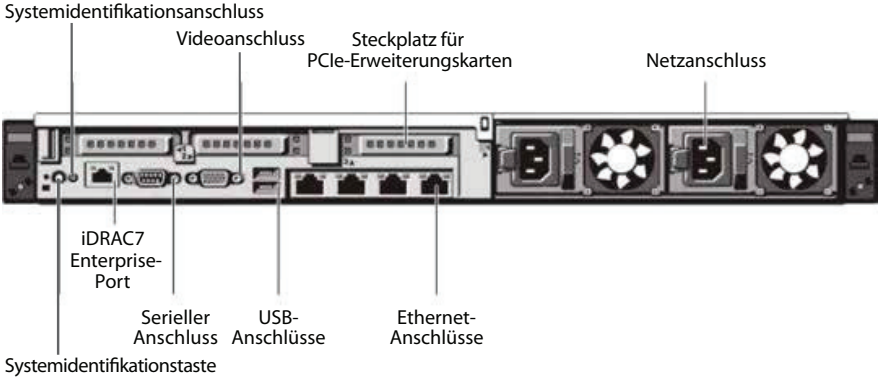
- Wenn der Switch nicht den eingehenden und den ausgehenden Datenverkehr spiegeln kann, müssen der gesamte Switch, alle VLANs (die das Senden/Empfangen ermöglichen) oder lediglich eine Schnittstelle (die das Senden/Empfangen zulässt) gespiegelt werden. Vergewissern Sie sich, dass Sie den zur Spiegelung verwendete Port nicht überlasten.
- Bei einigen Switches (z. B. Cisco 6509) muss möglicherweise zunächst die vorherige Portkonfiguration vollständig gelöscht werden, bevor neue Einstellungen vorgenommen werden können. In vielen Fällen entfernt der Switch die 802.1Q-Tags, wenn die alten Portinformationen nicht gelöscht werden.

3. Anschließen der Netzwerkkabel und erste Schritte

A. Auspacken der Appliance und Anschließen der Kabel

1. Nehmen Sie die Appliance und das Netzkabel aus der Verpackung.
2. Entfernen Sie den im Lieferumfang der Appliance enthaltenen Schienen-Bausatz.
3. Montieren Sie den Schienen-Bausatz an der Appliance und die Appliance im Rack.
4. Verbinden Sie die Netzwerkschnittstellen auf der Rückseite der Appliance über Netzwerkkabel mit den Switchports.

Beispiele für Schnittstellen auf der Rückseite — CounterACT-Appliance



B. Notieren der Schnittstellenzuweisungen

Nachdem Sie die Installation der Appliance im Rechenzentrum abgeschlossen und CounterACT Console installiert haben, werden Sie aufgefordert, die Schnittstellenzuweisungen anzugeben. Diese als *Kanaldefinitionen* bezeichneten Zuweisungen werden mit Hilfe des Assistenten für die Anfangseinstellungen (Initial Setup Wizard) eingegeben, der beim erstmaligen Anmelden bei Console geöffnet wird.

Notieren Sie sich in der folgenden Tabelle die Schnittstellenzuweisungen, um sie beim Durchführen der Kanalkonfiguration in Console schnell nachschlagen zu können.

Ethernet-Schnittstelle	Schnittstellenzuweisung (z. B. Verwaltung, Überwachung, Antwort)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

C. Einschalten der Appliance

1. Verbinden Sie das Netzkabel mit dem Netzanschluss auf der Rückseite der Appliance.
2. Schließen Sie das andere Ende des Kabels an eine geerdete Wechselstromsteckdose an.
3. Schließen Sie dann entweder eine Tastatur und einen Monitor an die Appliance an, oder konfigurieren Sie die Appliance für eine serielle Verbindung. Nähere Informationen erhalten Sie im *CounterACT Installation Guide (CounterACT-Installationshandbuch)* auf der CounterACT-CD.
4. Schalten Sie die Appliance auf der Vorderseite ein.

Wichtig: Schalten Sie den Computer stets aus, bevor Sie das Netzkabel abziehen.
Искључитемашинупре него што искључите

4. Konfigurieren der Appliance

Halten Sie die folgenden Informationen bereit, wenn Sie mit der Konfiguration der Appliance beginnen.

□ Hostname der Appliance	
□ CounterACT-Administratorkennwort	Bewahren Sie das Kennwort an einem sicheren Ort auf
□ Verwaltungsschnittstelle	
□ IP-Adresse der Appliance	
□ Netzwerkmaske	
□ IP-Adresse des Standardgateways	
□ DNS-Domänenname	
□ DNS-Serveradressen	

Nach dem Einschalten werden Sie mit folgender Meldung aufgefordert, die Konfiguration durchzuführen:

```
CounterACT Appliance boot is complete. (Starten der
  CounterACT-Appliance ist abgeschlossen.)
Press <Enter> to continue. (Drücken Sie zum
  Fortfahren die Eingabetaste.)
```

1. Öffnen Sie durch Drücken der **Eingabetaste** das folgende Menü:

```
1) Configure CounterACT (CounterACT konfigurieren)
2) Restore saved CounterACT configuration
   (Gespeicherte CounterACT-Konfiguration
   wiederherstellen)
3) Identify and renumber network interfaces
   (Netzwerkschnittstellen ermitteln und neu nummerieren)
4) Configure keyboard layout (Tastaturlayout
   konfigurieren)
5) Turn machine off (Computer ausschalten)
6) Reboot the machine (Computer neu starten)
Choice (1-6) :1 (Auswahl (1-6) :1)
```

2. Wählen Sie Option **1** – Configure CounterACT (CounterACT konfigurieren). Wenn die Aufforderung:

   `Continue: (yes/no) (Fortfahren: (Ja/Nein))?`

   erscheint, drücken Sie die **Eingabetaste**, um mit dem Einrichten zu beginnen.

3. Das Menü **`High Availability Mode (Hochverfügbarkeitsmodus)`** wird geöffnet. Wählen Sie durch Drücken der **Eingabetaste** die Standardinstallation aus.

4. Die Aufforderung **`CounterACT Initial Setup (CounterACT-Anfangseinstellungen)`** wird angezeigt. Drücken Sie zum Fortfahren die **Eingabetaste**.

5. Das Menü **`Select CounterACT Installation Type (CounterACT-Installationstyp auswählen)`** wird geöffnet. Geben Sie **1** ein, und drücken Sie dann die **Eingabetaste**, um die Standardinstallation der CounterACT-Appliance durchzuführen. Die Einstellungen werden initialisiert. Dies kann einige Zeit dauern.

6. Wenn die Aufforderung **`Enter Machine Description (Computerbeschreibung eingeben)`** erscheint, geben Sie einen kurzen beschreibenden Text für das Gerät ein, und drücken Sie dann die **Eingabetaste**.
   Die folgende Meldung wird angezeigt:

```
>>>>>> Set Administrator Password (Administratorken-
nwort festlegen) <<<<<<

This password is used to log in as 'root' to
the machine Operating System and as 'admin' to
the CounterACT Console. (Dieses Kennwort wird
benötigt, um sich als Root-Benutzer („root") beim
Betriebssystem des Computers und als Administrator
(„admin") bei CounterACT Console anzumelden.)
The password should be between 6 and 15 characters
long and should contain at least one non-alphabetic
character. (Das Kennwort muss zwischen 6 und
15 Zeichen lang sein und mindestens ein nicht-
alphabetisches Zeichen enthalten.)

Administrator password : (Administratorkennwort :)
```

7. Wenn die Aufforderung **`Set Administrator Password (Administratorkennwort festlegen)`** erscheint, geben Sie das gewünschte Kennwort (die eingegebene Zeichenkette wird auf dem Bildschirm nicht angezeigt) ein, und drücken Sie dann die **Eingabetaste**. Sie werden aufgefordert, das Kennwort zu bestätigen. Das Kennwort muss zwischen 6 und 15 Zeichen lang sein und mindestens ein nicht-alphabetisches Zeichen enthalten.
   Melden Sie sich an der Appliance als root *und bei Console als* admin an.

8. Wenn die Aufforderung **`Set Host Name (Hostname festlegen)`** erscheint, geben Sie den gewünschten Hostnamen ein, und drücken Sie dann die **Eingabetaste**. Der Hostname kann zur Anmeldung bei Console verwendet werden und wird in Console angezeigt, um Ihnen die Bestimmung der aktuell angezeigten CounterACT-Appliance zu erleichtern.

9. Im Fenster **`Configure Network Settings (Netzwerkeinstellungen konfigurieren)`** werden Sie aufgefordert, eine Reihe von Konfigurationsparametern einzustellen. Geben Sie für jeden Parameter einen Wert ein, und wechseln Sie dann durch Drücken der **Eingabetaste** zum nächsten Parameter.
   - Die Kommunikation zwischen den CounterACT-Komponenten erfolgt über Verwaltungsschnittstellen. Die Anzahl der aufgelisteten Verwaltungsschnittstellen ist abhängig vom jeweiligen Appliance-Modell.

- Die **Management IP address (IP-Adresse für die Verwaltung)** ist die Adresse der Schnittstelle, über die die CounterACT-Komponenten miteinander kommunizieren. Geben Sie für diese Schnittstelle nur dann eine VLAN-ID ein, wenn die für die Kommunikation der CounterACT-Komponenten verwendete Schnittstelle mit einem Port verbunden ist, auf dem VLAN-Tagging verwendet wird.
- Wenn unter **DNS server address (DNS-Serveradresse)** mehr als eine Adresse eingegeben werden muss, verwenden Sie jeweils ein Leerzeichen als Trennzeichen - Die meisten internen DNS-Server lösen externe und interne Adressen auf. Möglicherweise müssen Sie jedoch einen DNS-Server zum Auflösen externer Adressen hinzufügen. Da sich fast alle DNS-Anfragen der Appliance auf interne Adressen beziehen, sollte der DNS-Server für externe Adressen zuletzt eingegeben werden.

10. Das Fenster **`Setup Summary (Zusammenfassung der Konfiguration)`** wird angezeigt. Sie werden aufgefordert, entweder allgemeine Konnektivitätstests durchzuführen, Einstellungen neu zu konfigurieren oder das Einrichten abzuschließen. Geben Sie **D** ein, um die Konfiguration abzuschließen.

Lizenz

Nach der Installation müssen Sie die anfängliche Demolizenz installieren, die Sie von dem für Sie zuständigen CounterACT-Mitarbeiter erhalten haben. Die Lizenz wird während der Anfangseinstellungen für Console installiert. Diese anfängliche Demolizenz ist für eine gewisse Anzahl von Tagen gültig. Sie müssen vor Ablauf dieses Zeitraums eine permanente Lizenz installieren. Das genaue Ablaufdatum wird Ihnen in einer E-Mail mitgeteilt. Zudem werden in Console im Bereich „Appliances/Devices (Appliances/Geräte)“ ebenfalls Informationen zu Ablaufdatum und Statuslizenz angezeigt.

Nachdem Sie eine permanente Lizenz erhalten haben, wird diese Lizenz täglich durch den ForeScout-Lizenzserver validiert. Warnungen und Verstöße im Zusammenhang mit der Lizenz werden im Bereich „Device Details (Gerätedetails)“ angezeigt.

Lizenzen, die über einen längeren Zeitraum nicht validiert werden können, werden widerrufen. Weitere Informationen zu Lizenzen erhalten Sie im CounterACT-Installationshandbuch (CounterACT Installation Guide).

Anforderungen an die Netzwerkverbindung

Mindestens eines der CounterACT-Geräte (Appliance oder Enterprise Manager) muss auf das Internet zugreifen können. Über diese Verbindung validiert der ForeScout-Lizenzserver die CounterACT-Lizenzen.

Lizenzen, die über einen längeren Zeitraum nicht authentifiziert werden können, werden widerrufen. In diesem Fall sendet CounterACT einmal täglich eine Warnung per E-Mail, in der auf einen Kommunikationsfehler mit dem Server hingewiesen wird.

5. Remoteverwaltung

iDRAC7-Einrichtung

Integrated Dell Remote Access Controller 7 (iDRAC7) ist eine integrierte Serversystemlösung, die Ihnen unabhängig von Standort/Betriebssystem via LAN oder Internet den Remotezugriff auf Appliances/Enterprise Managers von CounterACT ermöglicht. Über das Modul erhalten Sie KVM-Zugriff und können Computer ein-/ausschalten und zurücksetzen sowie Aufgaben in Verbindung mit Fehlerbehebung und Wartung durchführen.

Für die Arbeit mit dem iDRAC-Modul sind die folgenden Schritte erforderlich:

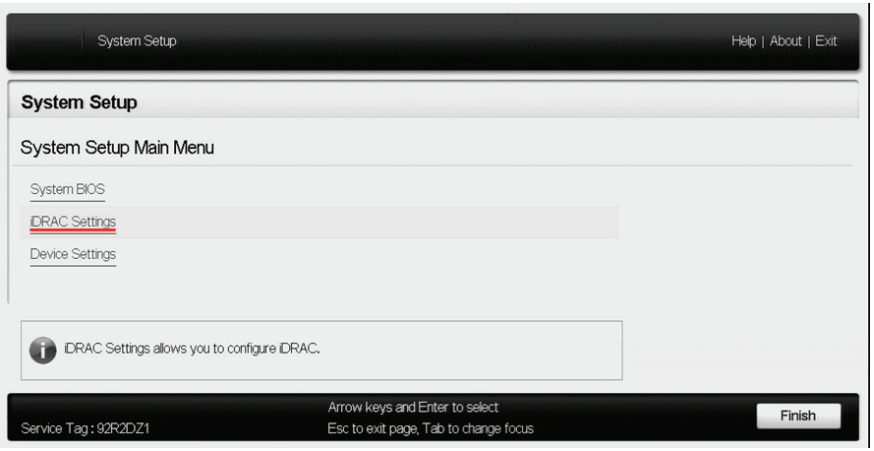
- *Aktivieren und Konfigurieren des iDRAC-Moduls*
- *Herstellen einer Verbindung zwischen Modul und Netzwerk*
- *Anmelden bei iDRAC*

Aktivieren und Konfigurieren des iDRAC-Moduls

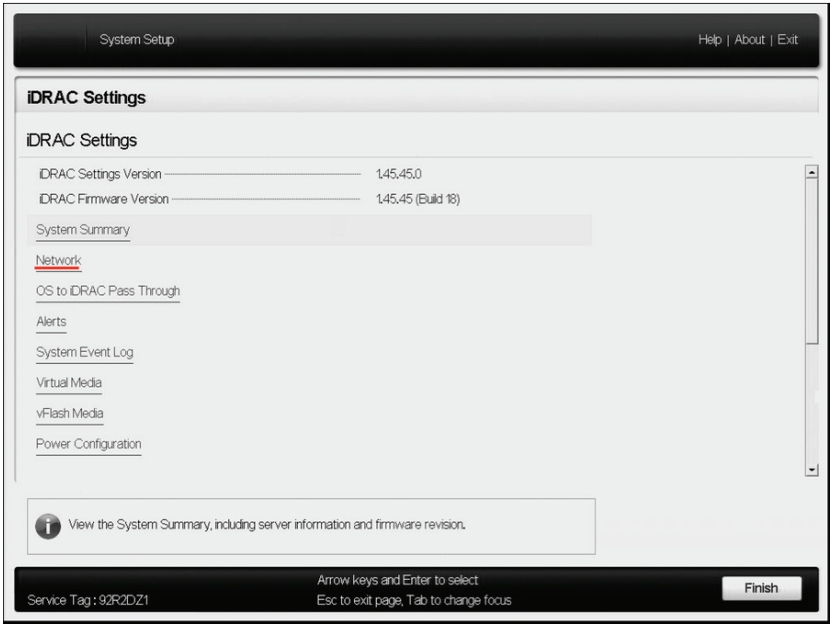
Ändern Sie die iDRAC-Einstellungen so, dass Remotezugriff auf das CounterACT-Gerät möglich ist. In diesem Abschnitt werden die grundlegenden Integrationseinstellungen für die Arbeit mit CounterACT beschrieben.

So konfigurieren Sie iDRAC:

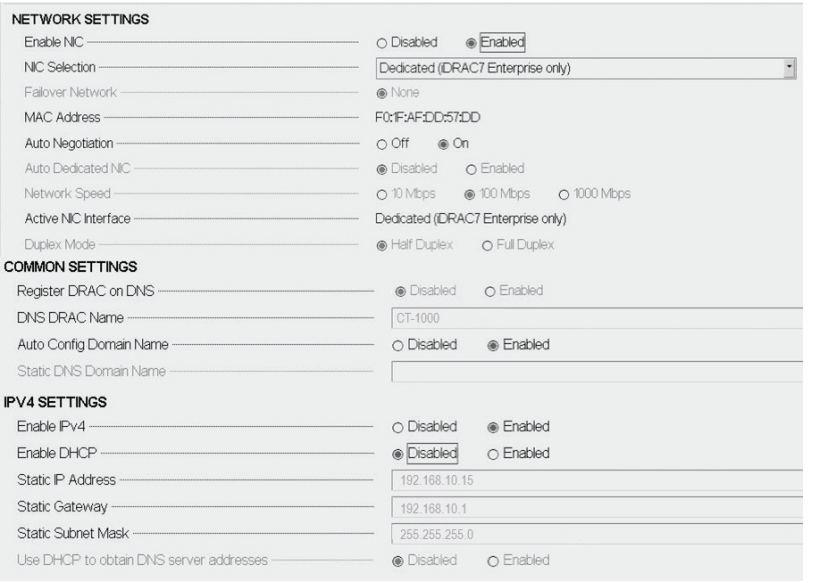
1. Aktivieren Sie das verwaltete System.
2. Drücken Sie während des Selbsttests (Power-on Self-test, POST) die F2-Taste.
3. Wählen Sie auf der Seite „System Setup Main Menu (Hauptmenü für die Systemeinrichtung)“ die Option **iDRAC Settings (iDRAC-Einstellungen)**.



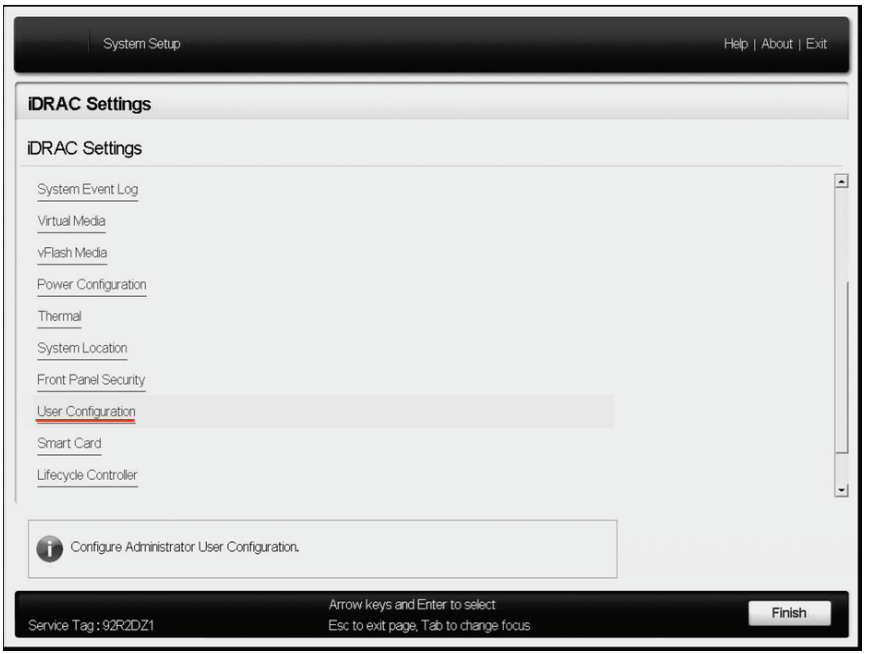
4. Wählen Sie auf der Seite „iDRAC Settings (iDRAC-Einstellungen)“ die Option **Network (Netzwerk)**.



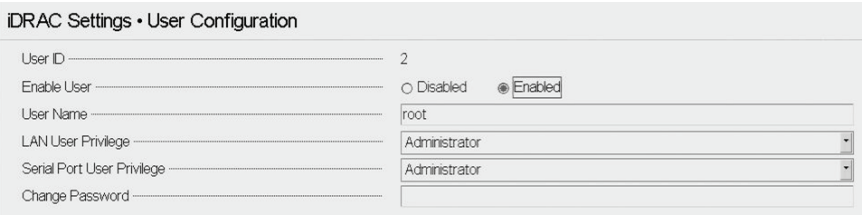
5. Konfigurieren Sie die folgenden Netzwerkeinstellungen:
   - ***Network Settings (Netzwerkeinstellungen).*** Vergewissern Sie sich, dass das Feld **Enable NIC (NIC aktivieren)** auf **Enabled (Aktiviert)** eingestellt ist.
   - ***Common Settings (Allgemeine Einstellungen).*** Im Feld „DNS DRAC Name (DRAC-Name im DNS)“ können Sie bei Bedarf die Informationen für ein dynamisches DNS aktualisieren.
   - ***IPV4 Settings (IPV4-Einstellungen).*** Vergewissern Sie sich, dass das Feld **Enable IPv4 (IPv4 aktivieren)** auf **Enabled (Aktiviert)** eingestellt ist.
     Wählen Sie unter **Enable DHCP (DHCP aktivieren)** entweder **Enabled (Aktiviert)**, um eine dynamische IP-Adressvergabe zu verwenden, oder „Disabled (Deaktiviert)“, wenn Sie statische IP-Adressen vergeben. Bei Aktivierung von DHCP werden iDRAC7 die IP-Adresse, das Gateway und die Subnetzmaske automatisch zugewiesen. Wenn DHCP deaktiviert ist, müssen Sie die entsprechenden Werte unter **Static IP Address (Statische IP-Adresse), Static Gateway (Statischer Gateway)** und **Static Subnet Mask (Statische Subnetzmaske)** manuell eingeben.



6. Wählen Sie dann **Back (Zurück)**.
7. Wählen Sie **User Configuration (Benutzerkonfiguration)**.



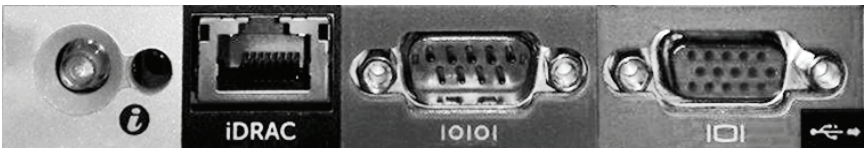
8. Konfigurieren Sie unter „User Configuration (Benutzerkonfiguration)“ die Einstellungen für die folgenden Felder:
    - ***Enable User (Benutzer aktivieren).*** Vergewissern Sie sich, dass dieses Feld auf „Enabled (Aktiviert)“ eingestellt ist.
    - ***User Name (Benutzername).*** Geben Sie einen Benutzernamen ein.
    - ***LAN User Privilege (Benutzerberechtigung für LAN) und Serial Port User Privilege (Benutzerberechtigung für seriellen Port).*** Wählen Sie für die Berechtigungsebenen jeweils „Administrator (Administrator)“ aus.
    - **Change Password (Kennwort ändern).** Legen Sie ein Kennwort fest, dass der Benutzer bei der Anmeldung eingeben muss.



9. Wählen Sie **Back (Zurück)** und dann **Finish (Fertig stellen)**. Bestätigen Sie die Änderungen der Einstellungen. Die Netzwerkeinstellungen werden gespeichert, und das System wird neu gestartet.

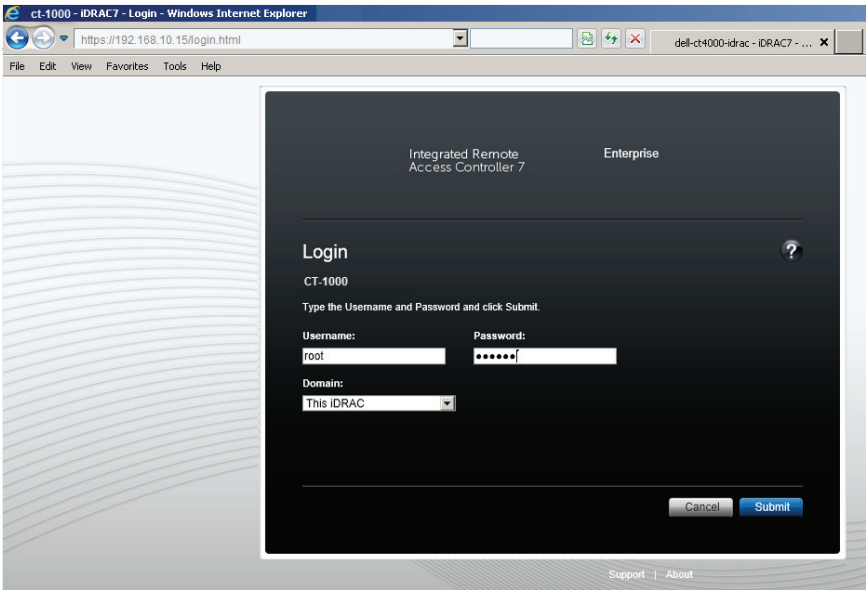
Herstellen einer Verbindung zwischen Modul und Netzwerk

iDRAC muss mit einem Ethernet-Netzwerk verbunden werden. Üblicherweise wird die Verbindung zu einem Verwaltungsnetzwerk hergestellt. Die nachfolgende Abbildung zeigt die Position des iDRAC-Ports auf der Rückseite der CT-1000-Appliance:



Anmelden bei iDRAC

So melden Sie sich bei iDRAC an:



1. Navigieren Sie zu der IP-Adresse oder dem Domänennamen, den Sie unter **iDRAC Settings > Network (iDRAC-Einstellungen > Netzwerk) konfiguriert haben.**
2. Geben Sie den Benutzernamen und das Kennwort ein, die Sie zuvor unter „User Configuration (Benutzerkonfiguration)“ im Einrichtungsmenü für das iDRAC-System festgelegt haben.
3. Wählen Sie dann **Submit (Senden)**.

Weitere Informationen zu iDRAC erhalten Sie im Benutzerhandbuch von iDRAC7.

Es ist äußerst wichtig, die Standardanmeldedaten zu ändern.

6. Prüfen der Verbindungen

Prüfen der Verbindung zur Verwaltungsschnittstelle

Um die Verbindung zur Verwaltungsschnittstelle zu testen, melden Sie sich an der Appliance an und führen Sie den folgenden Befehl aus:

```
fstool linktest
```

Die folgenden Informationen werden angezeigt:

```
Management Interface status (Status der
  Verwaltungsschnittstelle)
Pinging default gateway information (Pingtest für
  Standardgatewayinformationen durchführen)
Ping statistics (Pingstatistik)
Performing Name Resolution Test (Test für die
  Namensauflösung ausführen)
Test summary (Testzusammenfassung)
```

Prüfen der Verbindung zwischen Switch und Appliance

Überprüfen Sie, ob die Verbindung zwischen Switch und Appliance ordnungsgemäß funktioniert, bevor Sie das Rechenzentrum verlassen. Führen Sie dazu an der Appliance für jede erkannte Schnittstelle den Befehl **`fstool ifcount`** aus.

```
fstool ifcount eth0 eth1 eth2
```

(Trennen Sie die einzelnen Schnittstellen mit einem Leerzeichen.)

Dieses Tool zeigt fortwährend den Netzwerkdatenverkehr an den angegebenen Schnittstellen an. Es kann in zwei Modi verwendet werden: via Schnittstelle oder via VLAN. Der Modus kann über die Anzeige geändert werden. Neben der Gesamtanzahl von Bits pro Sekunde wird auch der Prozentsatz für jede der folgenden Datenverkehrkategorien angezeigt:

- Die Überwachungsschnittstelle sollte hauptsächlich gespiegelten Datenverkehr erkennen - über 90 %.
- Die Antwortschnittstelle sollte hauptsächlich Broadcast-Datenverkehr erkennen.
- Sowohl Überwachungs- als auch Antwortschnittstelle müssen die erwarteten VLANs erkennen.

Befehlsoptionen:

```
v – display in VLAN mode (Im VLAN-Modus anzeigen)
I – display in interface mode (Im
    Schnittstellenmodus anzeigen)
P – show previous (Vorheriges anzeigen)
N – show next (Nächstes anzeigen)
q – quit displaying (Anzeige beenden)
```

VLAN-Modus:

```
update=[4]   [eth3: 14 vlans] (aktualisieren=[4]   [eth3: 14 VLANs])

Interface/Vlan Total Broadcast Mirrored *To my MAC *From my MAC
(Schnittstelle/VLAN Gespiegelte Übertragung gesamt *An meine MAC-
Adresse *Von meiner MAC-Adresse)

eth3.untagged  4Mbps   0.2%    99.8%   0.0%    0.0%
(eth3.untagged  4 Mbit/s   0,2 %    99,8 %   0,0 %    0,0 %)

eth3.1     9Mbps   0.0%    100.0%   0.0%    0.0%
(eth3.1     9 Mbit/s   0,0 %    100,0 %   0,0 %    0,0 %)

eth3.2     3Mbps   0.1%    99.9%   0.0%    0.0%
(eth3.2     3 Mbit/s   0,1 %    99,9 %   0,0 %    0,0 %)

eth3.4     542bps  100.0%   0.0%    0.0%    0.0%
(eth3.4     542 Bit/s  100,0 %   0,0 %    0,0 %    0,0 %)

eth3.20     1Kbps   100.0%   0.0%    0.0%    0.0%
(eth3.20     1 Kbit/s   100,0 %   0,0 %    0,0 %    0,0 %)

Show [v]lans [i]nterfaces <-[p]rev [n]ext->     [q]uit ([v]VLANs [i]
Schnittstellen anzeigen <-[p]zurück [n]vor->     [q]beenden)
```

Schnittstellenmodus:

```
update=[31] [eth0: 32 vlans] [eth1: 1 vlans]
(aktualisieren=[31] [eth0: 32 VLANs] [eth1: 1 VLANs])

Interface Total Broadcast Mirrored *To my MAC *From my MAC
(Schnittstelle Gespiegelte Übertragung gesamt *An meine MAC-
Adresse *Von meiner MAC-Adresse)

eth0    3Kbps   42.3%   0.0%   14.1%    43.7%
 (eth0    3 Kbit/s   42,3 %   0,0 %   14,1 %    43,7 %)

eth1    475bps  0.0%    100.0%  0.0%    0.0%
(eth1    475 Bit/s  0,0 %    100,0 %  0,0 %    0,0 %)
```

*To my MAC (An meine MAC-Adresse) — MAC-Zieladresse entspricht der MAC-Adresse der Appliance.

*From my MAC (Von meiner MAC-Adresse) — Der von dieser Appliance gesendete Datenverkehr (MAC-Ausgangsadresse entspricht der MAC-Adresse der Appliance. Zieladresse kann Broadcast oder Unicast sein.).

Wenn kein Datenverkehr angezeigt wird, überprüfen Sie, ob die Schnittstelle einsatzbereit ist. Geben Sie an der Appliance den folgenden Befehl ein:

`ifconfig [interface name] up (ifconfig [Schnittstellenname] up)`

Durchführen des Pingtests

Für Sie zur Überprüfung der Verbindung einen Pingtest von der Appliance zu einem Netzwerkdesktop durch.

So führen Sie den Test durch:

1. Melden Sie sich bei der Appliance an.
2. Führen Sie den folgenden Befehl aus: **`Ping [network desktop IP] (Ping [Netzwerkdesktop-IP])`** Standardmäßig antwortet die Appliance selbst nicht auf die Ping-Anfrage.

7. Einrichten von CounterACT Console

Installieren von CounterACT Console

CounterACT Console ist eine zentrale Verwaltungsanwendung, mit der die von der Appliance erkannten Aktivitäten angezeigt, nachverfolgt und analysiert werden können. Über Console können Richtlinien zu NAC, Schutz vor Bedrohungen, Firewall und sonstigen Bereichen definiert werden. Weitere Informationen erhalten Sie im *CounterACT Console User Manual (CounterACT Console-Benutzerhandbuch)*.

Mindestanforderungen:

- Nicht-dedizierter PC, auf dem Windows NT/2000/2003/XP/Vista/7 oder Linux ausgeführt wird
- RAM
  1 GB für bis zu 10.000 Geräte
  2 GB für mehr als 10.000 Geräte
- Speicherplatz — 1 GB

Die Console-Anwendung kann auf zwei verschiedene Arten installiert werden:

Mit Hilfe der integrierten Installationssoftware Ihrer Appliance

1. Öffnen Sie auf dem Computer mit Console ein Browserfenster.
2. Geben Sie die folgende Adresse ein:
   `http://x.x.x.x/install`
   Wobei „x.x.x.x" der IP-Adresse Ihrer Appliance entspricht. Im Browser wird das Fenster für die Console-Installation geöffnet.
3. Befolgen Sie die Anweisungen auf dem Bildschirm.

Mit Hilfe der CounterACT-CD

1. Legen Sie die CounterACT-CD in das DVD-Laufwerk ein.
2. Öffnen Sie mit einem Browser die auf der CD enthaltene Datei **`ManagementSetup.htm`**.
3. Befolgen Sie die Anweisungen auf dem Bildschirm.

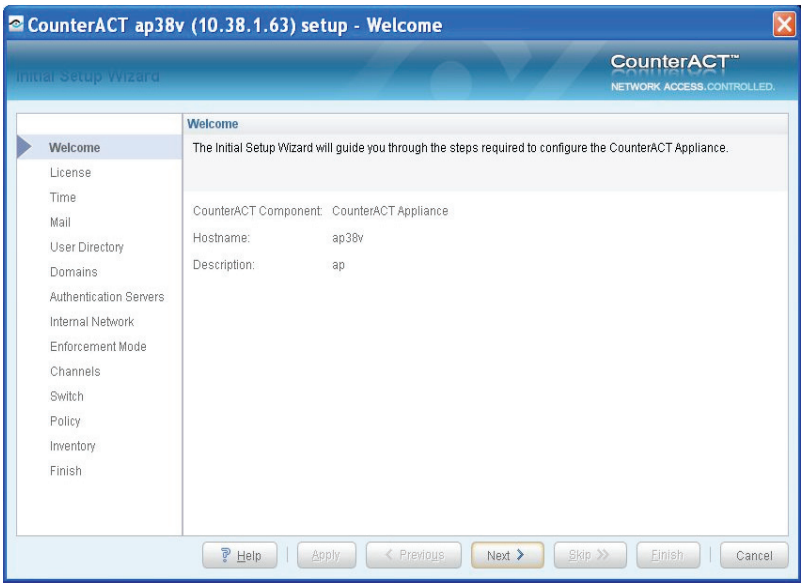
Anmelden

Nach Abschluss der Installation können Sie sich bei CounterACT Console anmelden.

1. Wählen Sie dazu das CounterACT-Symbol aus, dass Sie zuvor als Verknüpfung an dem von Ihnen gewünschten Speicherort erstellt haben.
2. Geben Sie im Feld **IP/Name (IP/ Name)** die IP-Adresse oder den Hostnamen der Appliance ein.
3. Geben Sie im Feld **User Name (Benutzername) admin** ein.
4. Geben Sie unter **Password (Kennwort)** das Kennwort ein, das Sie während der Installation der Appliance erstellt haben.
5. Wählen Sie **Login (Anmelden)**, um Console zu starten.

Durchführen der Anfangseinstellungen

Wenn Sie sich zum ersten Mal anmelden, wird der Assistent für die Anfangseinstellungen (Initial Setup Wizard) geöffnet. Der Assistent führt Sie durch die grundlegenden Konfigurationsschritte, damit CounterACT schnell einsatzbereit ist und effizient ausgeführt wird.



Vor Beginn der Anfangseinstellungen

Halten Sie die folgenden Informationen bereit, wenn Sie mit dem Assistenten beginnen.

Informationen	Werte
□ Adresse des von Ihrem Unternehmen verwendeten NTP-Servers (optional).	
□ IP-Adresse für die interne E-Mail-Weiterleitung. Dies ermöglicht das Senden von E-Mails aus CounterACT, wenn die Appliance keinen SMTP-Datenverkehr zulässt (optional).	
□ E-Mail-Adresse des CounterACT-Administrators.	
□ Die im Rechenzentrum festgelegten Zuweisungen für Überwachungs- und Antwortschnittstelle.	
□ Für Segmente oder VLANs ohne DHCP benötigen Sie das Netzwerksegment oder die VLANs, mit denen die Überwachungsschnittstelle direkt verbunden ist, sowie eine permanente IP-Adresse für jedes VLAN, das mit CounterACT verwendet wird. Diese Informationen werden zum Einrichten von Enterprise Manager nicht benötigt.	
□ IP-Adressbereiche, die durch die Appliance geschützt werden (alle internen Adressen, einschließlich nicht verwendeter).	
□ Kontoinformationen für das Benutzerverzeichnis und die IP-Adresse des Servers mit dem Benutzerverzeichnis.	
□ Anmeldedaten für die Domäne, einschließlich Kontoname und Kennwort für die Domänenadministration.	
□ Authentifizierungsserver, damit CounterACT analysieren kann, welche Netzwerkhosts erfolgreich authentifiziert wurden.	
□ IP-Adresse, Anbieter- und SNMP-Parameter des Coreswitches.	

Weitere Informationen zur Arbeit mit dem Assistenten erhalten Sie im *CounterACT Console User Manual (CounterACT Console-Benutzerhandbuch)* oder in der Online-Hilfe.

Kontaktinformationen

Wenden Sie sich bei Problemen per E-Mail unter support@forescout.com oder per Telefon unter einer der folgenden Rufnummern an den technischen Support von ForeScout:

- Gebührenfrei (USA): 1.866.377.8771
- Telefon (International): 1.408.213.3191
- Support: 1.708.237.6591
- Fax: 1.408.371.2284

Abbildungen mit freundlicher Genehmigung der Dell Corporation.

©2014 ForeScout Technologies, Inc. Produkte geschützt durch folgende US-Patente: 6,363,489; 8,254,286; 8,590,004 und 8,639,800. Alle Rechte vorbehalten. ForeScout Technologies und das ForeScout-Logo sind Marken von ForeScout Technologies, Inc. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber. Die Nutzung jedes ForeScout-Produkts unterliegt den Bedingungen des Endbenutzer-Lizenzvertrags von ForeScout, der unter www.forescout.com/eula eingesehen werden kann.

ForeScout Technologies
900 E. Hamilton Ave., Suite 300
Campbell, CA 95008 USA

Gebührenfrei: 1.866.377.8771
Telefon (International):
1.408.213.3191
www.forescout.com

400-00020-00